

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Area around 3324-3326 North 50 Street, Milwaukee,
Wisconsin - See Attachment A

Case No. 19-M-182

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Section 844(i)

The application is based on these facts: See attached affidavit.

- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

ATF Special Agent Rick Hankins

Printed Name and Title

Sworn to before me and signed in my presence:

Date: July 24, 2019



Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones

U.S. Magistrate Judge

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Rick Hankins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under Title 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Special Agent of the U.S. Department of Justice's Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed since April 2003. My duties as a Special Agent with the ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as the ATF National Academy. That training included various legal courses related to constitutional law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as interviewing, surveillance, and evidence collection.

4. In addition to my duties as a criminal investigator, I am also an ATF Certified Fire Investigator (CFI). As an ATF CFI, I am tasked with providing expert opinions as to the origin

and cause of fires. I obtained the ATF CFI certification in 2009 following a two-year training program that centered on various fire science topics including, but not limited to: chemistry, fire dynamics, and building construction. The two-year ATF CFI certification program consisted of college courses, written exams, research papers, reading assignments, practical training exercises, and test burns of various materials. I am re-certified annually as an ATF CFI. To date, I have participated in over 260 fire scene examinations and have testified as an expert. Additionally, I have been certified as a fire investigator by the International Association of Arson Investigators since June 2011. I have received over 1,200 class hours of fire-related training. Furthermore, I have been an instructor regarding fire-related topics on multiple occasions for the following agencies and institutions: The National Fire Academy (FEMA), International Association of Arson Investigators Chapter 25, Waukesha County Technical College, and Blackhawk Technical College. I have also participated in over 200 live fire training exercises, where I started training fires and observed fire growth and development. Finally, I was a full-time instructor at the ATF National Academy from approximately August 2015 to August 2016, where I taught several topics during Special Agent Basic Training for new ATF recruits. Specifically, I was a primary instructor for the arson block of training at the ATF Academy.

5. This affidavit is based upon my personal knowledge as well as information provided to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon information gathered from interviews of citizen witnesses, reports, official records, law enforcement reports, and my training and experience.

6. I am an investigative or law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18, United States Code, in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

7. As a part of my duties with the ATF, I investigate criminal violations relating to arson and arson-related offenses, including violations of Title 18, United States Code, Section 844. During the course of my investigations, I have regularly used data forensically extracted from cellular devices to obtain evidence relating to the commission of criminal offenses, including intent, motive, manner, means, and the identity of co-conspirators.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 844(i) (maliciously damaging or destroying by means of fire or explosive any building used in interstate commerce) has been committed by an Unknown Suspect. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by Title 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” Title 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

10. Based on my training and experience, I know that cellular devices, such as mobile telephones, are widely-used wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part

of the cellular network called “cell sites,” which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

11. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet (“Wi-Fi”) access points if a user enables Wi-Fi connectivity. Wi-Fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the Wi-Fi network. In general, devices with Wi-Fi capability routinely scan their environment to determine what Wi-Fi access points are within range and will display the names of networks within range under the device’s Wi-Fi settings.

12. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device’s transmission range, to which it might connect.

13. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system (“GPS”) technology. Using this

technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

14. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

15. In addition, based on my training and experience, I know that Google is offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google), online file storage (including Google Drive, Google Photos, and Youtube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and Youtube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account.

16. In addition, based on my training and experience, I know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browsing software, although Chrome can also be used without

signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices.

17. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

18. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about Wi-Fi access points and Bluetooth beacons within range of the mobile device.

19. Based on my training and experience, I also know that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and

app- based activity and associates this information with the Google account associated with the Android device and/or that is signed in with the relevant Google app.

20. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google accounts those devices are associated with. Among other things, this information can inculcate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

21. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

22. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the

status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

Fires at 3324-3326 North 50th Street, Milwaukee, WI

23. On April 8, 2019, at approximately 3:17am, the Milwaukee Fire Department (MFD) responded to a fire at 3324-3326 North 50th Street in the City of Milwaukee, Wisconsin ("**Target Location**"). The property is a two-story structure that is used as residential rental property and was occupied at the time of the fire. An occupant of the residence and a neighbor heard the sound of glass breaking at the time of the fire. The subsequent investigation revealed the fire originated on the outside of the structure on or near the rear living room window. There were no accidental heat sources located in the area of origin and an odor of a petroleum distillate was observed. The Milwaukee Fire Department classified this fire as incendiary.

24. On April 11, 2019, at approximately 8:42pm, MFD again responded to a fire at the Target Location. A resident at the Target Location observed an unknown person fleeing the rear of the residence as a fire was burning on the outside of the structure on and near the kitchen window. From the fire investigation, it appears that an unknown person broke the kitchen window and set the window blinds on fire. This fire was also classified as incendiary.

25. I have reviewed the MFD and other law enforcement reports regarding the April 8 and 11 fires at the Target Location. Based on those reports, my investigation, and my arson training and experience, I believe that there is probable cause that unknown person(s) maliciously and intentionally started the fires at the Target Location.

CONCLUSION

34. Based on the forgoing, there is probable cause to believe that unknown suspects set incendiary fires, in violation of 18 U.S.C. § 844(i), at 3324-3326 North 50th Street on April 8, 2019, and April 11, 2019.

35. I further submit that there is probable cause to search information in the possession of Google relating to what devices were in the Target Location described in Attachment A during the time period described in Attachment A, as well as information that identifies the Google accounts with which those devices are associated, for evidence of the crimes at issue in this case. Among other things, this information can inculcate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation. The Target Location and times correspond to the fires described above.

36. In order to facilitate the manageable disclosure of and search of this information, the proposed warrant contemplates that Google will disclose the information to the government in stages rather than disclose all of the information for which the government has established probable cause to search at once. Specifically, as described in Attachment B.I:

- a. Google will be required to disclose to the government an anonymized list of devices that specifies information including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported

their location within the Target Location described in Attachment A during the time period described in Attachment A.

- b. The government will then review this list in order to prioritize the devices about which it wishes to obtain associated information.
- c. Google will then be required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquires.

37. I therefore request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c).

38. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

39. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC and applies to:

- (1) location history data, sourced from methods including GPS, wi-fi, and Bluetooth, generated from devices and that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google Accounts associated with the responsive location history data.

Search Parameters

Location: Area Around 3324-3326 North 50th Street, Milwaukee, Wisconsin

Date: 04/08/2019 / Time Period (including time zone): 0245hrs(CST) – 0330hrs(CST)

Date: 04/11/2019 / Time Period (including time zone): 2015hrs(CST) – 2055hrs(CST)

Target Location: Geographical area identified within the following latitude/longitude coordinates and connected by straight lines:

- Point 1: 43.079973°N, - 87.974887°W
- Point 2: 43.079640°N, - 87.974887°W
- Point 3: 43.079632°N, - 87.975599°W
- Point 4: 43.080006°N, - 87.975565°W



ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

Google shall provide responsive data (as described in Attachment A) to the government pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A.
2. For each location point recorded within the Initial Search Parameters, Google shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").
3. The government shall review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information.
4. Google is required to disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each device ID about which the government inquires.

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 844(i) that were committed on or about January 10 and February 1, 2019 involving the residences at 4047 N. 7th Street, Milwaukee, WI, and 5915 N. 42nd Street, Milwaukee, WI.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE
902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is _____ . I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature